OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

Semester 2 Examinations 2023/2024

Course Instance Code(s)	4BCT, 1MECE, 1OA, 1EM
Exam(s)	B.Sc. (Computer Science & Information Technology), M.E. (Electronic and Computer Engineering)
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
External Examiner(s)	Dr. Ramona Trestian
Internal Examiner(s)	Prof. Michael Madden *Dr. Michael Schukat

Instructions: **Answer any four questions.**
All questions carry equal marks.

Duration	**2 hours**
No. of Pages	**4**
Discipline(s)	Computer Science
Course Co-ordinator(s)	Dr. Effirul Ramlan

Requirements:

Release in Exam Venue	No[ ]	Yes [☑]
MCQ Answer sheet	No [☑]	Yes [ ]
Handout	No [☑]	Yes [ ]
Formulae & Tables*	No [☑]	Yes [ ]
Cambridge Tables 2nd Edition**	No [☑]	Yes [ ]
Graph Paper*** A4 Graph Paper 1mm 0.1cm Squared (Standard)	No [☑]	Yes [ ]
Other Materials	No [☑]	Yes [ ]
Graphic material in colour	No [☑]	Yes [ ]

End of requirements.

Question 1 (15 Marks)

a) Assume you operate a distributed network of sensors to monitor the water quality of lakes and rivers in Co. Galway. The battery-operated sensors are resource-constrained (also in terms of their memory footprint / CPU performance), and use wireless networks (e.g., Wi-Fi, 4G) to transmit sensor readings to a datacentre in Oranmore.
Considering all the above constraints, determine the most efficient solution to provide for data integrity of the **transmitted sensor readings using a hash function, in order to prevent data manipulation** by a MitM. Use a diagram to support your answer.

[10 marks]

b) Distinguish between the terms **true random number generator**, **pseudo-random number generator**, and **pseudo-random function**. Provide diagrams to support your answer.

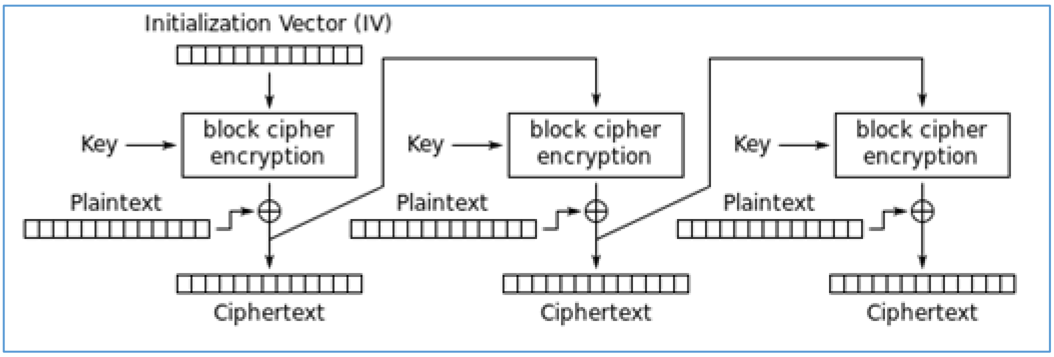
[5 marks]

Question 2 (15 Marks)

a) In the context of block ciphers, what is meant by the term **mode of operation**?
Identify the mode of operation shown in the diagrams below and draw a diagram that shows the corresponding data decryption process.
Further on, determine if this mode supports:

- Parallelisable encryption
- Parallelisable decryption
- Random read access of individual blocks for decryption.

[9 marks]



b) Operating system kernels and network protocol stacks may be vulnerable to buffer overflow attacks if they are implemented in the "C" programming language.
Using examples show how such attacks can happen and suggest to what extent they can be detected and avoided.

[6 marks]

PTO

Question 3 (15 Marks)

a) Digital certificates are normally used to bind a public key to an identity. However, this technology could also be used to implement a digital vaccination travel certificate. Such a certificate would be issued by a healthcare provider to vaccinated travellers and stored on their mobile phones. A 3rd party (e.g., border control) would subsequently read and validate the certificate to determine if and when its owner completed which vaccination (e.g., hepatitis A, tetanus or typhoid).

Further elaborate on this idea, thereby outlining

- a suitable internal certificate structure (that may contain features of attribute extension fields or attribute certificates),
- an architecture and method to issue, validate, and to revoke such a certificate.

Fully explain your design, using diagrams where appropriate.

[9 marks]

b) Using diagrams where appropriate, distinguish between the following IPSec-related terms / concepts:

a. Tunnel mode versus transport mode
b. Anti-replay window
c. Combining security associations

[6 marks]

Question 4 (15 Marks)

a) Distinguish between the terms **timing attack** and **unsafe function**.
Explain why the function below is unsafe and suggest code improvements.

```
bool isNumberInArray(int number, int *array, int arrayLength) {
   int i;
   for (i = 0; i < arrayLength; i++)
               if (number == array[i])
                     return true;
   return false;
```

[6 marks]

b) Using diagrams show how data encryption / decryption is achieved with Double-DES and Triple-DES. Evaluate, to what extent both algorithms are vulnerable to a **meet-in-the-middle attack**.

[9 marks]

PTO

Question 5 (15 Marks)

a) Explain the following (TLS-related) terms, using diagrams where appropriate:

- OCSP Stapling
- Version rollback attack
- Certificate path validation
- The key share Extension
- Mutual authentication

[5 marks]

b) Using examples, explain the concept and the inner workings of a **Feistel cipher**, a **SP network**, and its components (i.e., **S-boxes** and **P-boxes**).
Further on explain, how a Feistel cipher can be combined with a SP network, and from there further expanded to a Feistel network, in order to build a block cipher.

[10 marks]

Question 6 (15 Marks)

a) Using diagrams to support your answer, distinguish between and explain the inner workings of:

- a LFSR
- a combined LFSR
- a NLFSR

[6 marks]

b) Discuss in some detail, if and how **message authentication** (potentially in combination with a message sequence number) can prevent the following attacks on data communication:

- (Sender) Masquerade
- Denial-of-Service
- Content modification
- Sequence modification
- Timing modification

[9 marks]

END OF EXAM